PATENT ABSTRACTS OF JAPAN

(11)Publication number : 63-063232
(43)Date of publication of application : 19.03.1988

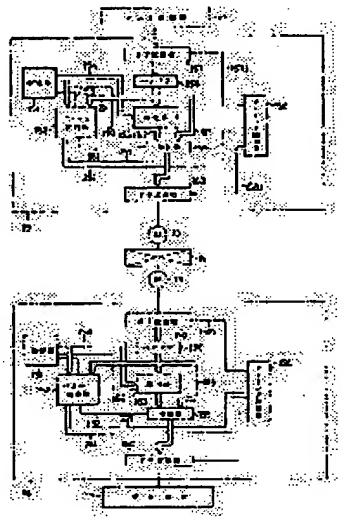
(51)Int.Cl. H04L 9/00

(21)Application number : 61-206855
(22)Date of filing : 04.09.1986

(71)Applicant : OKI ELECTRIC IND CO LTD
(72)Inventor : SAKAMOTO SHUNICHIRO

(54) CIPHERED COMMUNICATION SYSTEM

(57)Abstract:
PURPOSE: To cipher even a packet switching network by ciphering from the next byte of a telegram through its end only when pattern data in the telegram agrees with pattern data which is set and inputted to an input means.
CONSTITUTION: Telegram data from a host computer 11 is set to a buffer 156 through an SP converter 157. Telegram data from the buffer 156 is inputted to a pattern detector 152, a ciphering device 153 and a switch 159. Without a switching signal from the pattern detector 152, the switch 159 outputs not- ciphered telegram data that is inputted through a data line 163, and transmits it to a line (a network 14) through a MODEM 13. When the pattern detector 152 detects that both pattern data are the same, the switching signal is outputted through a signal line 161, and the switch 159 selects an output line 162 from the ciphering device 153. The ciphering device 153 ciphers data from the host computer 11, and an PS converter 160 transmits it to the MODEM 13 and the network 14 through the switch 159. 12 terminal equipment 151 setting device 158 timing control part 164 decoding device.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

⑲日本国特許庁（JP）　⑪特許出願公開

⑫公開特許公報（A）　昭63－63232

⑤Int.Cl.⁴　識別記号　庁内整理番号　⑬公開　昭和63年(1988)3月19日
H 04 L 9/00　Z－7240－5K

審査請求　未請求　発明の数 1　（全15頁）

⑭発明の名称　暗号化通信方式

⑳特　願　昭61－206855
㉒出　願　昭61(1986)9月4日

㉒発明者　坂本　俊一郎　東京都港区虎ノ門1丁目7番12号　沖電気工業株式会社内
㉑出願人　沖電気工業株式会社　東京都港区虎ノ門1丁目7番12号
㉔代理人　弁理士　鈴木　敏明

明　細　書

1．発明の名称

暗号化通信方式

2．特許請求の範囲

回線における電文データを暗号化して通信する暗号化通信方式において、

パターンデータを設定して入力するための入力手段と、

前記電文データ中のパターンデータと前記入力手段に設定入力されたパターンデータを比較する比較手段と

を備え、

前記比較手段で前記パターンデータが互いに一致したときに、前記電文データ中の前記パターンデータの次のバイトデータから終了のバイトデータまでを暗号化して通信する

ことを特徴とする暗号化通信方式。

3．発明の詳細な説明

〔産業上の利用分野〕

本発明は通信回線における電文データの秘密保護に係り、特にこの電文データを暗号化して通信する暗号化通信方式に関するものである。

〔従来の技術〕

従来、このような分野の技術としては、例えば特開昭５８－２１３５４４号公報に示されるものがあった。このような従来装置においては、回線上を流れるデータの保護のため暗号装置を回線に入れることが行なわれている。

第２図は回線における電文データを暗号化する場合に適用されている従来システムの接続図である。暗号装置１はホスト計算機２とモデム４の間および端末装置３とモデム４の間に設けられる。なお、同図において、モデム４の間に設けられているのは交換網５である。通常この型の暗号装置は、回線が接続されると送受信データ（電文データ）を常に暗号化／復号化するようにしている。

第１４図は送信電文（同図（ａ））と、暗号電

文（同図（ｂ））と、それを復号した受信電文（同図（ｃ））の構成例を示す図である。この例では、最初のフレームのＡ部（アドレスフィールド）以後をすべて暗号化している、すなわち、ホスト計算機２あるいは端末装置３からの送信電文（第１４図（ａ）図示）を送信側の暗号装置４で最初のＡ部から暗号化し、回線へは暗号電文（第１４図（ｂ）図示）を送出している。この暗号電文を受信した受信側の暗号装置４はこれを復号化して受信電文（第１４図（ｃ）図示）とし、これをホスト計算機２あるいは端末装置３に渡している。

このため、回線の種類が専用回線、公衆回線等であっても、一度接続されると電文データの内容にかかわらず送信データをそのまま伝送する回線に対しては、従来の暗号装置を適用することは可能である。しかし、例えばパケット交換網のパケット交換サービスを利用しようとした場合には、網に対して接続手順（Ｘ２５、ＣＡＬＬ）およびデータ転送手順（Ｘ２５、ＤＡＴＡ）を行う必要がある。この手順では、第１５図に示す様にパケット内のパケットヘッダに制御情報があり、このパケットを網との間でデータをやり取りすることにより通信が行なわれている。

ところが、従来の暗号装置における暗号化通信方式では、第１４図（ｂ）に示す様に暗号化開始後はすべてのＦ部（フラグ）、Ａ部（アドレスフィールド）、Ｃ部（コントロールフィールド）、データ部を暗号化してしまうため、網において接続手順、データ転送手順に必要なデータを認識することが出来ない。このため、従来の暗号化通信方式をパケット交換網に適用することができないという問題があった。

そこで本発明は、パケット交換網等の如く、網と端末／ホストとの間で接続手順、データ転送手順がある場合にも適用可能な暗号化通信方式を提供することを目的とする。

〔問題点を解決するための手段〕

本発明に係る暗号化通信方式は、所定のパターンデータを設定入力する入力手段と、電文データ中のパターンデータと入力手段に設定入力されたパターンデータを比較する比較手段とを備え、比較手段でパターンデータが互いに一致したときに電文データ中のパターンデータの次のバイトデータから終了のバイトデータまでを暗号化して通信することを特徴とする。

〔作用〕

本発明の暗号化通信方式は以上のように構成されるので、入力手段は監視のためのパターンデータを設定入力するように働き、比較手段は監視のために設定入力されたパターンデータと送られる電文データ中のパターンデータを比較し、暗号化して通信されるデータか否かを監視するように働き、従って比較手段における比較結果にもとづいて暗号化すべきデータのみを暗号化して通信するように働く。

〔実施例〕

以下、添付図面の第１図、第３図ないし第１３図を参照して本発明のいくつかの実施例を説明する。

第１図は本発明の第１の実施例に係る暗号化通信方式を適用する通信システムの構成図である。同図において、ホスト計算機１１と端末装置１２の間の通信は、２つのモデム１３とこれらの間に接続される網１４を介してなされる。また、ホスト計算機１１側には本実施例の要部をなす暗号装置の暗号化部１５が接続され、端末装置１２側には同じく本実施例の要部をなす復号化部１６が接続される。なお、第１図はホスト計算機１１から端末装置１２への通信の例を示しており、従って端末装置１２からホスト計算機１１への通信を行なう場合には、上記と同様のものを逆方向に配置すればよい。

次に、暗号化部１５の構成を第１図に従って説明する。暗号化部１５はパターンデータと暗号化キーを設定するための設定器１５１を有し、ここで設定されたパターンデータは信号線１５４を介してパターン検出器１５２および暗号器１５３に与えられる。また、暗号化部１５はホスト計算機１１からのシリアルな電文データをパラレル信号

に変換するためのＳＰ変換器１５７と、ここで変換された電文データを一時記憶するバッファ１５６を有し、バッファ１５６の内容は信号線２９を介してパターン検出器１５２に与えられると共に、信号線１６３を介して暗号器１５３および切替器１５９に与えられる。

切替器１５９は暗号器１５３からの暗号化されたデータを信号線１６２を介して受けると共に、バッファ１５６から送信された暗号化されていないデータを信号線１６３を介して受ける。そして、切替器１５９はパターン検出器１５２からの信号線１６１による出力に応じてこれらデータを切り替え、暗号化れたデータ又は暗号化されていないデータのいずれかをＰＳ変換器１６０に出力する。タイミング制御部１５８はＳＰ変換器１５７からの信号を信号線１５７１を介して受け、信号線２１４によるバイトクロックと信号線２２１による電文中信号でパターン検出器１５２の動作を制御すると共に、信号線１５８１を介してＰＳ変換器１６０の動作タイミングをも制御する。

次に、復号化部１６の構成を第１図に従って説明する。復号化部１６の構成は暗号化部１５の構成と基本的に同一である。異なる点は、暗号器１５３に代えて復号器１６４が設けられていることのみである。

次に、第３図を参照して第１図に示すパターン検出器１５２の詳細な構成を説明する。このパターン検出器１５２はパターンデータメモリ２１と、カウンタ２２と、ＡＮＤゲート２３と、比較器２４と、フリップフロップ（Ｆ／Ｆ）２５とを主たる構成要素とする。

まず、第１図に示すバッファ１５６からの暗号化されていない電文データは信号線２９を介してＡＮＤゲート２３に与えられる。第１図中のタイミング制御部１５８からの電文中信号は信号線２２１を介してカウンタ２２およびＦ／Ｆ２５の反転入力端子に与えられ、バイトクロックは信号線２１４を介してＡＮＤゲート２１５に与えられる。第１図中の設定器１５１からのパターンデータ書込信号は信号線１５５を介してＯＲゲート２７に与えられると共に、パターンデータメモリ２１にも与えられる。さらに、設定器１５４からのパターンデータは信号線１５４を介してパターンデータメモリ２１のデータ入力端子に与えられる。

カウンタ２２はＯＲゲート２７の出力信号をカウントし、信号線２２１からの電文中信号によりリセットされる。そして、カウンタ２２は出力をパターンデータメモリ２１のアドレス入力端子Ａに与える。パターンデータメモリ２１は信号線１５５からのパターンデータ書込信号に応じて信号線１５４からのパターンデータを入力する。そして、データ線２１１によりマスクデータをＡＮＤゲート２３に与えると共に、データ線２１２を介して比較データを比較器２４に与える。また、パターンデータメモリ２１は信号線２１３を介して終了信号をＡＮＤゲート２６に与えると共に、これをインバータを介してＡＮＤゲート２１５に与える。Ｆ／Ｆ２５の出力は信号線２５１を介してＡＮＤゲート２６に与えられ、ＡＮＤゲート２６の出力は切替信号として信号線２８から第１図の切替器１５９に与えられる。

第４図は第３図に示すパターンデータメモリ２１の詳細構成図である。図示の如く、パターンデータメモリ２１は１７ビット×ｎワード構成の書込可能なメモリを使用し、上位８ビットをマスクデータＭ、次の８ビットを比較データＣ、最後の１ビットを終了フラグとして使用している。

次に、第５図を参照して第１図に示す暗号器１５３の詳細な構成を説明する。同図（ａ）の如く、暗号器１５３は暗号化キーがＫ１からＫ４までの４個のキーレジスタ３１と、４個のＥＸＯＲ回路３２と、f_1 から f_3 までの３個の換字用ＲＯＭ３４を主たる要素とする。第５図（ｂ）、（ｃ）は換字用ＲＯＭ３４の構成の一例を示すもので、アドレスが８ビット、データが８ビットの計２５６バイトのＲＯＭである。このような換字変換ＲＯＭ３４によれば、例えば第５図（ｃ）の様にデータを書き込んでおくことにより、アドレスの００はデータの０１へ、アドレスの０１はデ

ータのＥ４へと換字変換される。

このように構成される暗号器１５３によれば、入力された平文データ（暗号化されていないデータ）はＥＸＯＲ回路３２でキーレジスタ（Ｋ１）３１のキーＫ１と排他的論理和がとられる。次に、換字用ＲＯＭ（f_1）３４で換字変換され、さらにキーレジスタ（Ｋ２）３１のキーＫ２と排他的論理和がとられる。以下同様にして、最終的にはキーレジスタ（Ｋ４）３１のキーＫ４と換字用ＲＯＭ（f_4）３４の出力との排他的論理和が暗文データ（暗号化されたデータ）となる。

第１図に示す復号器１６４の構成も上記暗号器１５３と同様で、暗文データと平文データの流れる方向を逆にすれば良い。

次に、上記の如く構成される第１の実施例に係る暗号化通信方式を適用した装置の作用を説明する。

まず、暗号化通信動作をさせる前には暗号装置を初期設定する必要がある。この初期設定は次のように行なう。すなわち、第１図の設定器１５１によりパターン検出器１５２内のパターンデータメモリ２１にマスクデータＭ、比較データＣ、終了フラグを設定し、つぎに暗号器１５３の４個のキーレジスタ３１にそれぞれ暗号キーＫ１，Ｋ２，Ｋ３，Ｋ４を設定する。同様に、端末装置１２側の復号化部１６のパターン検出器１５２、復号器１６３にも上記と同様の設定をする。

上記の初期設定が終ると、次にパターンデータの設定を行なう。これは、例えば第６図および第７図に示すように行なう。すなわち、第６図（ａ）に示す送信電文中のD_1～D_5の部分のみを暗号化する場合には、第７図に示すパターンをパターンデータメモリ２１に設定する。このようにすると、暗号化された暗号電文は第６図（ｂ）に示すようになり、復号化された受信電文は第６図（ｃ）に示すようになる。

次に、暗号化／復号化動作を説明する。まずホスト計算機１１からの電文データはＳＰ変換器１５７によりバイト単位のデータに変換される。このとき、第６図に示す同期パターン（Ｆ）、フレームチェックシーケンス（ＦＣＳ）は除去される。

次に、ＳＰ変換器１５７から最初のデータがバッファ１５６にセットされ、制御線１５７１によりタイミング制御部１５８にデータ受信開始を通知する。タイミング制御部１５８は信号線２２１，２１４を介してパターン検出器１５２へ電文中信号とバイトクロックを出力する。

次に、バッファ１５６からの電文データはパターン検出器１５２、暗号器１５３および切替器１５９にそれぞれ入力される。パターン検出器１５２からの切替信号（信号線１６１）がないときは、切替器１５９はデータ線１６３を介して入力される暗号化されない電文データを出力している。切替器１５９の出力はＰＳ変換器１６０によりシリアル変換され、同期パターン（Ｆ）、フレームチェックシーケンス（ＦＣＳ）を付加されてモデム１３を介して回線（網１４）に送出される。

パターン検出器１５２から信号線１６１を介して切替信号が出力されるまでは、ＰＳ変換器１６０へはバッファ１５６のデータがそのまま与えられる。パターン検出器１５２によりパターンデータの一致が検出されると、信号線１６１を介して切替信号が出力され、切替器１５９は暗号器１５３からの出力線１６２を選択する。この後、ホスト計算機１１からのデータは暗号器１５３により暗号化され、切替器１５９を介してＰＳ変換器１６０によりモデム１３、網１４に送信される。

ホスト計算機１１からの電文データ出力の終了はＳＰ変換器１５７で検出され、制御線１５７１によりタイミング制御部１５８に通知される。タイミング制御部１５８はパターン検出器１５２への信号線２２１による電文中信号をＯＦＦとしてパターン検出動作をリセットし、制御線１５８１により電文データの終了をＰＳ変換器１６０に通知する。ＰＳ変換器１６０では電文データの終了としてフレームチェックシーケンス（ＦＣＳ）、終結フラグを付加し、電文データの送出を終了する。

端末装置１２側の復号化部１６においても以上

説明したと同様に動作するが、バッファ１５６の出力を復号器１６４を通して切替器に入力することのみ異なっている。

次に、上記作用におけるパターン検出器１５２の動作を、第３図、第６図および第７図を用いて説明する。なお、第６図（ａ）の送信電文の５．１部分は、すでにパターンデータメモリ２１に書き込まれているものとする。

最初のバイトＡ部がＳＰ変換器１５７からバッファ１５６にセットされると、タイミング制御部１５８から信号線２２１．２１４を介して電文中信号とバイトクロックがパターン検出器１５２に出力される。信号線２１４のバイトクロックはＳＰ変換器１５７でバイト単位に変換されるたびに制御信号線１５７１を通じてタイミング制御部１５８に入力され、そこからパターン検出器１５２に入力される。

カウンタ２２は信号線２２１の電文中信号によりリセットが解除され、パターンデータメモリ２１のアドレス入力端子Ａにアドレス０を出力している。パターンデータメモリ２１のアドレス０の内容のうち、マスクデータＭ＝ＦＦはデータ線２１１に、比較データＣ＝５５はデータ線２１２に、終了フラグ＝０は終了信号線２１３に出力されている。この状態で、バッファ１５６から信号線２９を介して電文データがＡＮＤゲート２３に入力される。このＡＮＤゲート２３で、データ線２１１からのマスクデータＭと論理積が取られ、この場合はマスクデータＭがＦＦであるので信号線（データ線）２９の電文データがそのまま比較器２４に入力される。

比較器２４ではパターンデータメモリ２１の比較データＣ（信号線２１２からのデータ）と比較され、その結果が信号線２４１を介してＯＲゲート２７に出力される。信号線２４１には両者が一致した場合に０が出力され、一致しない場合に１が出力される。Ｆ／Ｆ２５とＯＲゲート２７はこの状態を記憶している。すなわち、比較器２４の出力線２４１が０であればＦ／Ｆ２５の出力線２５１は１のままであるが、１度でも比較器２４の出力線２４１が１となるとＦ／Ｆ２５の出力線２５１は０となる。

ここで、第１バイトが一致した場合はＦ／Ｆ２５の出力線２５１は１となっているが、パターンデータメモリ２１の終了信号線２１３は０であるため、ＡＮＤゲート２６によりゲートされて切替信号は信号線２８を介して出力されない。

次に、第２バイトの受信時は、信号線２１４のバイトクロックによりＯＲゲート２７を通してカウンタ２２にクロックが与えられ、カウンタ２２の出力はアドレス１を示すことになる。これにより、パターンデータメモリ２１のアドレス１の内容と信号線２９の電文データが比較されることになる。以下同様にして、各電文データと比較される。

ここで第６バイト目の比較時には、パターンデータメモリ２１のアドレス部にアドレス５が入力されている。この場合、パターンデータメモリ２１の終了信号線２１３は１であるため、Ｆ／Ｆ２５の出力線２５１が１であればＡＮＤゲート２６が開き、切替信号が信号線２８を介して出力される。つまり、ここまでの電文データがすべて一致していれば、終了信号線２１３が１になったとき切替信号が信号線２８から出力される。これにより以降のデータは暗号化されることとなる。

また、終了信号線２１３が１になるまでに電文データが１バイトでも不一致であると、Ｆ／Ｆ２５の出力線２５１が０となるため切替信号は信号線２８を介して出力されることがない。このため、それ以降も暗号化されない電文データが送信される。また、この終了信号線２１３によりＡＮＤゲート２１５を閉じて以降のバイトクロックをゲートする。

この様にして各電文データを比較し、パターンデータの一致した電文データの次のバイトから電文の終了までを暗号化する。マスクパターンＭは電文データ中の通番等、各電文データ毎に変化するものをマスクするのに使用する。

この第１の実施例ではホスト／端末とモデムの間に暗号装置を設け、電文の一部のみの暗号化を

行なっている。このため、ホスト／端末からの電文を一度シリアルパラレル変換し、暗号化の後に再度パラレルシリアル変換している。ところが、以下に示す第２の実施例は、暗号機能を通信制御装置中にもたせている。

第８図乃至第１３図を参照して、本発明の第２の実施例を説明する。

第８図は本発明に係る暗号化通信方式の第２の実施例に適用される通信制御装置の構成を示すブロック図である。通信制御装置８０は制御用プロセッサ（μＰ）８１と、このプロセッサ８１に付設される制御メモリ（ＣＭ）８２と、チャネルインタフェース８３ａと、このチャネルインタフェース８３ａに付設されるチャネルバッファ８３ｂと、データメモリ（ＤＭ）８４と、暗号／復号器（ＣＩＰ）８５と、設定器８６と、４個の回線ユニット（ＬＡ＃０～ＬＡ＃３）８７とを有し、これらの間ではバスを介して互いにデータの授受ができるようになっている。

第９図は上記第２の実施例で用いられる回線コントロールメモリの構成図である。そして、このメモリは各回線毎に設けられている。このメモリの内容は、通信制御用データ９１と、暗号処理用データ９２と、復号処理用データ９３とを有している。

通信制御用データ９１は従来の通信制御装置のものと同様で、通信速度、同期方式等の回線の情報である。このデータは第８図に示すＣＰＵにより設定される。暗号処理用データ９２はこの回線の送信データを暗号化するか否かのＥＣフラグと、現在暗号化中であることを示すＥＩフラグと、暗号化キーＥＫＥＹ０～ＥＫＥＹ３と、暗号化する電文データであるか否かを判定するためのマスクデータおよび比較データと、その管理用ポインタＥＰ、ＥＭとからなる。このうち、ＥＣ、ＥＫＥＹ０～ＥＫＥＹ３、ＥＭ、暗号マスクデータ、復号比較データは第８図における設定器８６により設定される。ＥＩ、ＥＰの初期値は０である。

復号処理用データ９３はこの回線の受信データを復号するか否かのフラグＤＣと、現在復号化中であることを示すフラグＤＩと、復号化キーＤＫＥＹ０～ＤＫＥＹ３と、復号化する電文データであるか否かを判定するためのマスクデータおよび比較データと、その管理用ポインタＤＰ、ＤＭとからなる。このうちＤＣ、ＤＫＥＹ０～ＤＫＥＹ３、ＤＭ、復号マスクデータ、復号比較データは第８図の設定器８６により設定される。またＤＩ、ＤＰの初期値は０に設定される。

第１０図は第８図に示す暗号／復号器８５の詳細な構成図である。暗号化キーレジスタ１０１はＥＫＥＹ０～ＥＫＥＹ３、の４個からなり、暗号化キーレジスタ１０１へのセット信号は信号線１０２から与えられる。暗号化用データラッチ１０３と、f_1～f_3の３個の暗号換字ＲＯＭ１０５は排他的論理和手段１０４に結ばれ、最後の排他的論理和出力は暗号化データ出力用のゲート１０６を介して出力される。

復号化キーレジスタ１０７はＤＫＥＹ０～ＤＫＥＹ３の４個からなり、復号化キーレジスタ１０７へのセット信号は信号線１０８を介して与えられる。復号化用データラッチ１０９と$\bar{f}_3$～$\bar{f}_1$の３個の復号換字ＲＯＭ１１０は排他的論理和手段１０４により結ばれ、最後の排他的論理和出力は復号化データ出力用のゲート１１１を介して出力される。

ここで、復号換字ＲＯＭ１１０は暗号換字ＲＯＭ１０５の逆変換を行なう内容をもっている。

次に、第８図乃至第１０図に示す第２の実施例の作用を説明する。

第１１図は第８図に示す通信制御装置におけるデータの処理を示すフローチャートである。この処理は、第８図に示す制御プロセッサ８１が制御メモリ８２に書き込まれた内容に従って動作することにより行なわれる。

制御用プロセッサ８１は動作開始後、チャネル要求チェック（ステップ３０１）とＬＡ要求チェック（ステップ３０３）を常に行なっている。チャネル要求チェック（ステップ３０１）で要求有りの場合には、チャネルコマンド処理（ステップ

３０２）へ行きＣＰＵからのコマンド（例えば送信要求、受信要求）の処理を行なう。ＬＡ要求チェック（ステップ３０３）で要求チェック有りの場合には、ＬＡ選択（ステップ３０４）でどの回線ユニットＬＡからの要求かを判別し、第９図に示す回線コントロールメモリのアドレスを得る。

次に、送信／受信チェック（ステップ３０５）でＬＡからの要求が送信か受信かを判別し、送信の場合には送信終了チェック（ステップ３０５）で送信データがすべて送信し終ったかどうか判断する。終了であった場合には、送信終了処理（ステップ３０８）でＬＡに対する終結処理（例えばフレームの終了）と回線コントロールメモリのイニシャライズを行う。終了でなかった場合には、ＬＡ出力（ステップ３０７）で第８図に示すチャネルインタフェース８３ａに付設されたチャネルバッファ８３ｂからＬＡへデータを出力する。このとき、後述の方法によりデータを暗号化するか否かの判断と暗号化処理を行なう。

送信／受信チェック（ステップ３０５）において受信要求であった場合には、受信終了チェック（ステップ３０９）で受信が終了したかどうかの判別を行う。終了であった場合には、受信終了処理（ステップ３１１）でＬＡすなわち回線ユニットのリセットと回線コントロールメモリの初期化を行い、終了でなかった場合にはＬＡ入力（ステップ３１０）でＬＡからデータを読み出し、第８図に示すチャネルインタフェース８３ａに付設されたチャネルバッファ８３ｂのデータをセットする。このとき、そのデータを復号化するか否かの判別を行うと共に、復号化する場合にはその復号処理を行なう。

第１２図は第１１図のＬＡ出力処理（ステップ３０７）およびＬＡ入力処理（ステップ３１０）の詳細を示すフローチャートである。

まず、ＬＡ出力について第１２図（ａ）を参照して説明する。ＬＡ出力はステップ４０１でチャネルバッファ８３ｂから送信データを取り出すことにより始まる。

次に、暗号化する送信データであるか否かを示すＥＣビットをチェックする（ステップ４０２）。そして、ＥＣ＝０である場合には、この回線は暗号化を行なわない回線としてステップ４１３に行き、送信データをそのままＬＡにセットする。ＥＣ＝１でかつＥＩ＝１の場合には暗号化を適用する回線として、ステップ４１２で送信データを暗号化した後、ステップ４１３でＬＡにセットする。

ステップ４０３でＥＩ＝０の場合には、次のステップ４０４で管理用ポインタＥＰとＥＭを比較する。そして、ＥＰ＝ＥＭであった場合にはこの電文はすでに暗号化対象外であると判別されているので、送信データをそのままでＬＡにセットする（ステップ４１３）。ステップ４０４でＥＰ≠ＥＭの場合には、ステップ４０５でまずＥＰの指すマスクデータと比較データを、第９図の回線コントロールメモリ内の暗号処理用データ９２から得る。

ステップ４０６で送信データとマスクパターンとの論理積を取り、ステップ４０７でその値と比較データを比較する。一致しない場合はＥＰをＥＭの値とし（ステップ４０８）、この電文を暗号対象外として送信データをＬＡにセットする（ステップ４１３）。一致した場合にはＥＰに１を加算し（ステップ４０９）、再度ＥＰとＥＭを比較する（ステップ４１０）。

ステップ４１０でＥＰとＥＭが一致の場合には、第９図の暗号処理用データ９２内の比較データがすべて一致したことになり、ＥＩフラグを１にセットし（ステップ４１１）、次の送信データから暗号化を行う。不一致の場合にはステップ４１１の処理を行なわず、ＬＡに送信データをセットする（ステップ４１３）。

この様にして送信電文の比較チェックを行ない、一致検出後の電文データのみ暗号化を行なう。電文データの終了時は第１１図のステップ３０８の送信終了処理でＥＩフラグおよびＥＰを０にリセットし、次の電文チェックを可能にする。

ＬＡ入力の処理は第１２図（ｂ）に示す通りであるが、第１２図（ａ）のＬＡ出力処理と略同一

である。すなわち、ＬＡ入力はステップ４１４のＬＡからのデータ入力処理と、ステップ４１５の復号処理と、ステップ４１６のチャネルバッファへの受信データセットがＬＡ出力処理と異なるのみで、ＥＣ，ＥＩ，ＥＰ，ＥＭをそれぞれＤＣ，ＤＩ，ＤＰ，ＤＭと読み替えれば全く同様の処理である。

第１３図は第１２図（ａ）に示す暗号化処理（ステップ４１２）と、同図（ｂ）に示す復号化処理（ステップ４１５）の詳細は処理を示すフローチャートである。

第１３図（ａ）の暗号化処理ではまず、ステップ５０１で暗号化キーレジスタ１０１へ第９図の暗号処理用データ９２のＥＫＥＹ０～ＥＫＥＹ３をセットする。次に、ステップ５０３で暗号化したいデータを第８図の暗号化用データラッチ１０３にセットする。これにより第５図で説明したと同様にして、暗号化されたデータが暗号化データ出力ゲートに出力される。そして、ステップ５０４で暗号化出力ゲート１０６からデータを読む。

同様に第１３図（ｂ）の復号化処理においても、ステップ５０５で復号化キーレジスタ１０７へ復号処理用データ９３のＤＫＥＹ０～ＤＫＥＹ３をセットする。次に、ステップ５０３で復号化したいデータを第８図の復号化用データラッチ１０９にセットする。そして、ステップ５０７で復号化されたデータを復号化データ出力ゲート１１１から読み出す。

本発明は上記第１および第２の実施例に限定されるものではなく、種々の変形が可能である。例えば第１図、第３図、第５図の等の回路構成は一例であって、各要素のは他の要素で置換することができる。

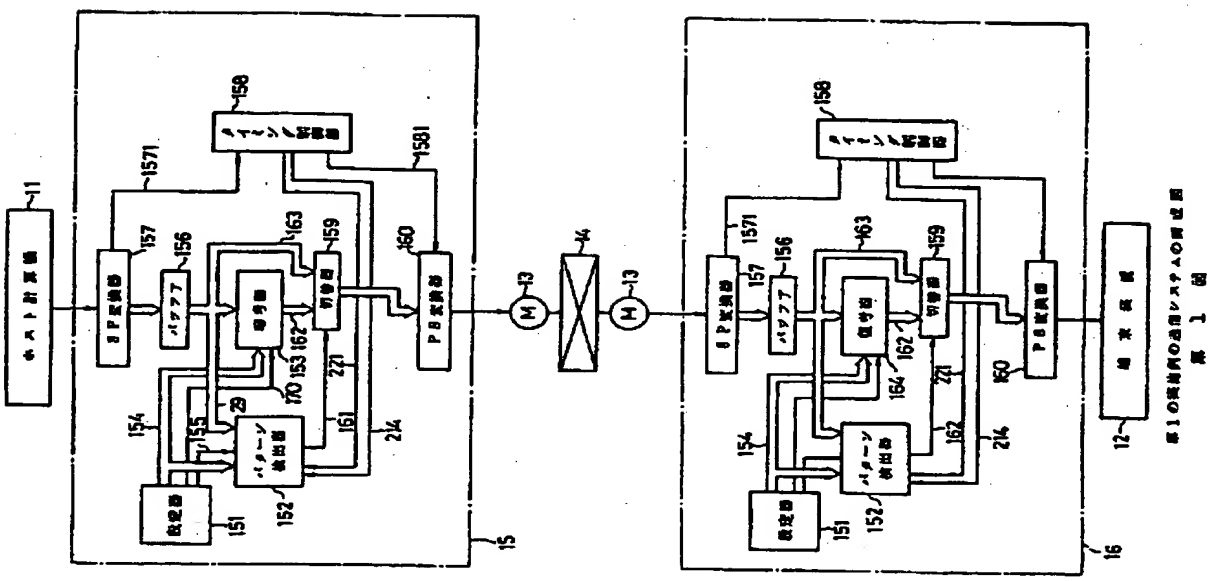
〔発明の効果〕

以上、詳細に説明した様に本発明によれば、暗号化する電文の監視のためのパターンデータを入力する入力手段を設け、電文中のパターンデータが上記入力手段に設定入力されたパターンデータと一致した場合のみその電文の次のバイトから電文の終了までを暗号化する様にしたので、網との間で手順に必要なデータ部はそのまま平文で網に通知することが可能となり、従って網と端末／ホストとの間で手順を必要とするパケット交換網に対しても暗号化を適用することができる。

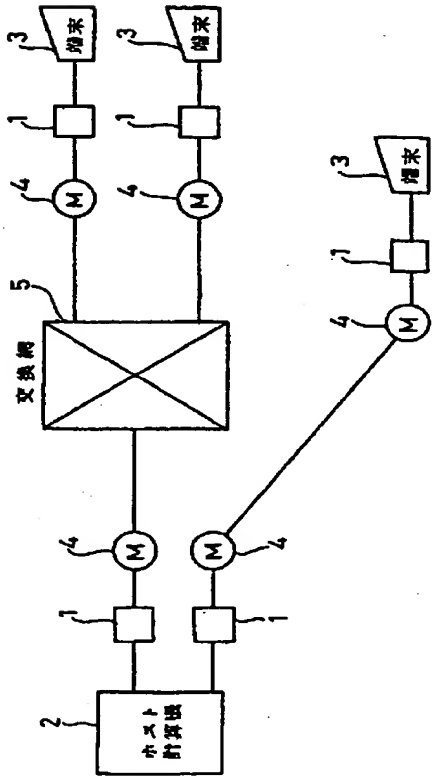
４．図面の簡単な説明

第１図は本発明方式の第１の実施例に係る暗号化通信方式を備えた通信システムの構成図、第２図は従来の暗号化通信方式を備えた通信システムの接続形態を示す構成図、第３図は第１図に示すパターン検出器の詳細な構成を示す図、第４図は第３図に示すパターンデータメモリの詳細な構成図、第５図は第１図に示す暗号器の詳細な構成図、第６図は第１の実施例による送受信電文と暗号化電文の構成図、第７図は第４図のパターンデータメモリに設定されるパターンデータの説明図、第８図は本発明方式の第２の実施例に係る暗号化通信方式を備えた通信システムの構成図、第９図は第２の実施例に用いられる回線コントロールメモリの構成図、第１０図は第８図に示す暗号／復号器の詳細な構成図、第１１図は第８図の装置におけるデータ処理を示すフローチャート、第１２図は第１１図のＬＡ出力処理およびＬＡ入力処理の詳細を示すフローチャート、第１３図は第１２図の暗号化処理と復号化処理の詳細を示すフローチャート、第１４図は従来方式による送受信電文と暗号電文の構成図、第１５図はパケットの構成図である。

１５…暗号化部、１６…復号化部、３１…キーレジスタ、３２…ＥＸＯＲ回路、３４…換字用ＲＯＭ、８０…通信制御装置、８１…制御用プロセッサ、８２…制御メモリ、８３ａ…チャネルインタフェース、８３ｂ…チャネルバッファ、８４…データメモリ、８５…暗号／復号器、８７…回線ユニット、１０１…暗号化キーレジスタ、１０４…排他論理和手段、１０５…暗号換字ＲＯＭ、１０７…復号化キーレジスタ、１１０…復号換字ＲＯＭ。

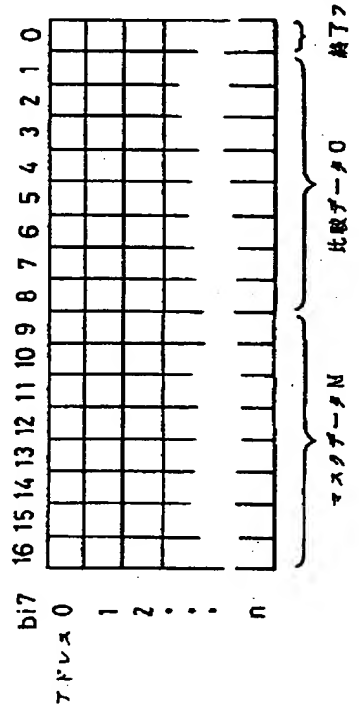


第1図



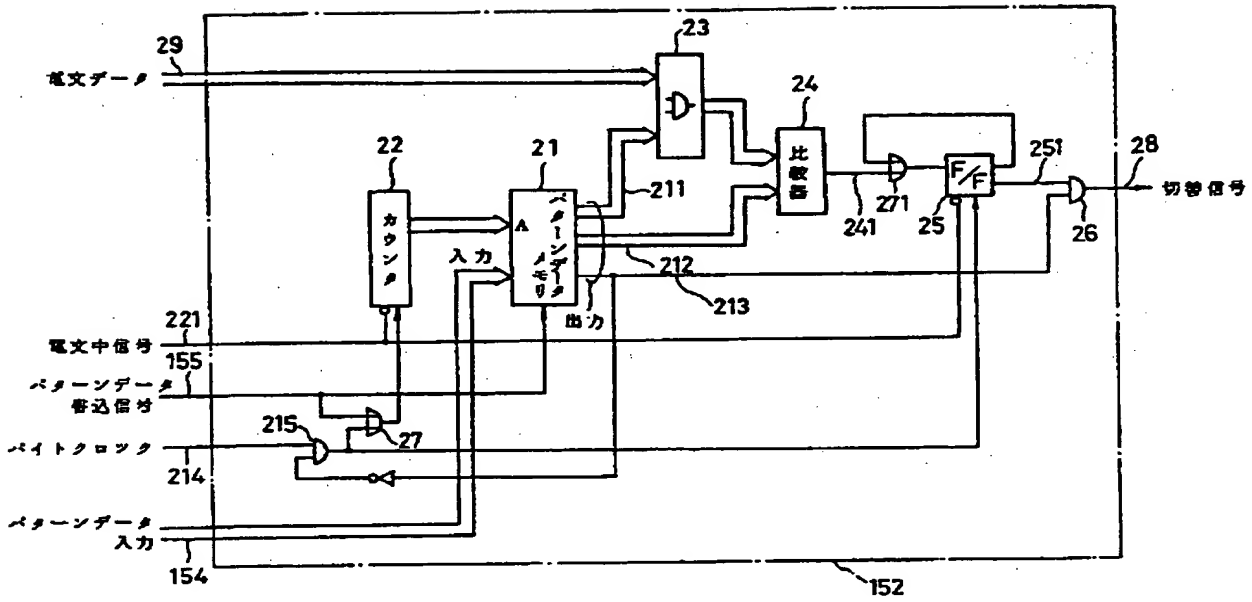
従来方式による時分割接続形態を示す図

第2図



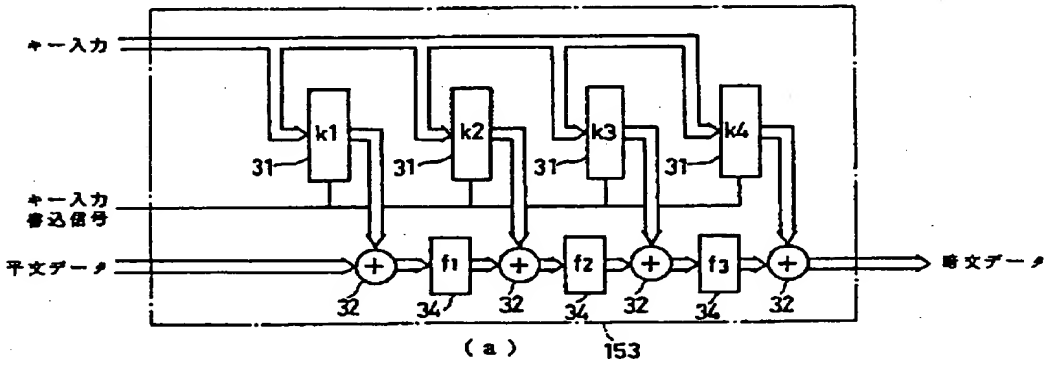
第3図のパターンデータメモリの構成図

第4図

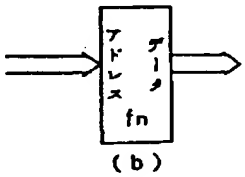


第1図のパターン検出器の構成図

第 3 図



(a)



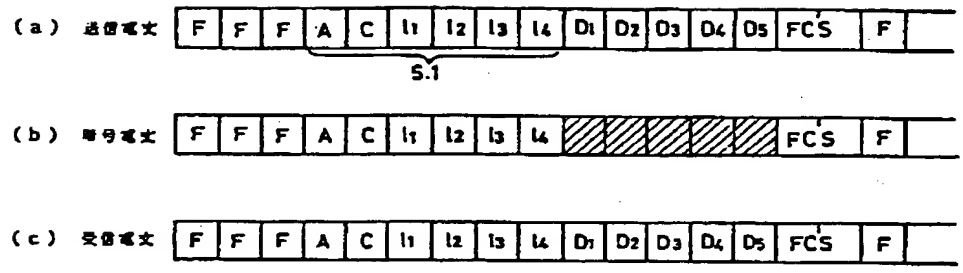
(b)

アドレス	データ
00	01
01	E4
02	18
⋮	⋮
FF	08

(c)

第1図の暗号器の構成図

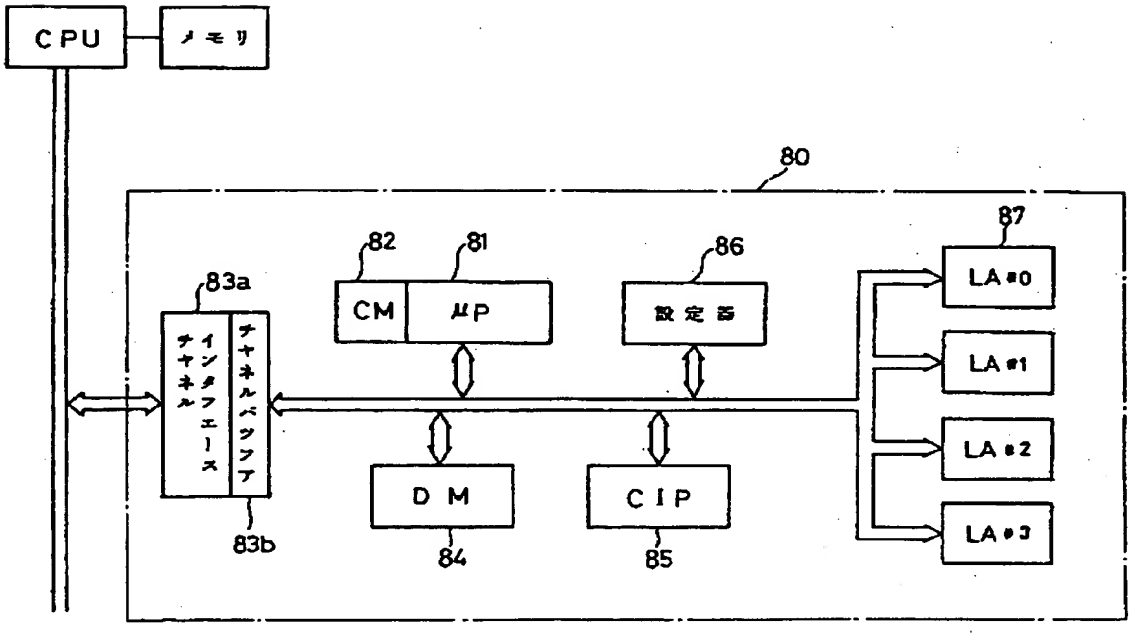
第 5 図



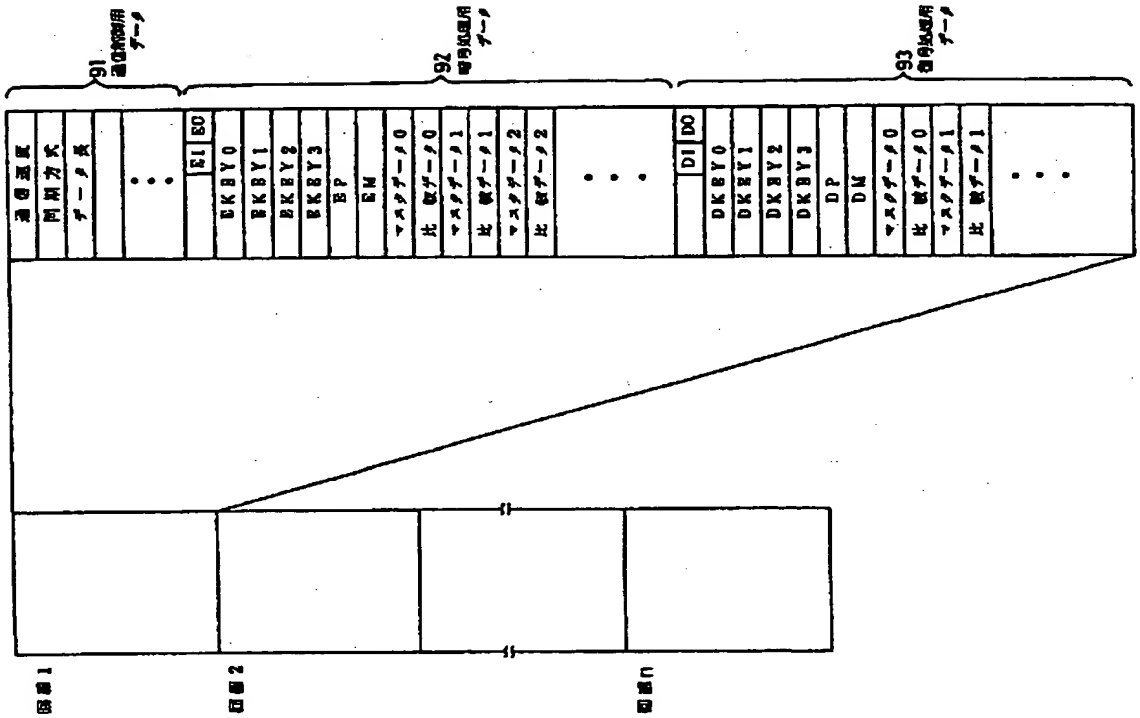
第1の実施例による送受信電文と受信電文
第 6 図

アドレス				
0	FF_H	55 (A)	0
1	01	00 (C)	0
2	70	20 (I1)	0
3	00	00 (I2)	0
4	01	00 (I3)	0
5	00	00 (I4)	1
	マスクデータM	比較データD	終了フラグ

パターンデータメモリ例の説明図
第 7 図

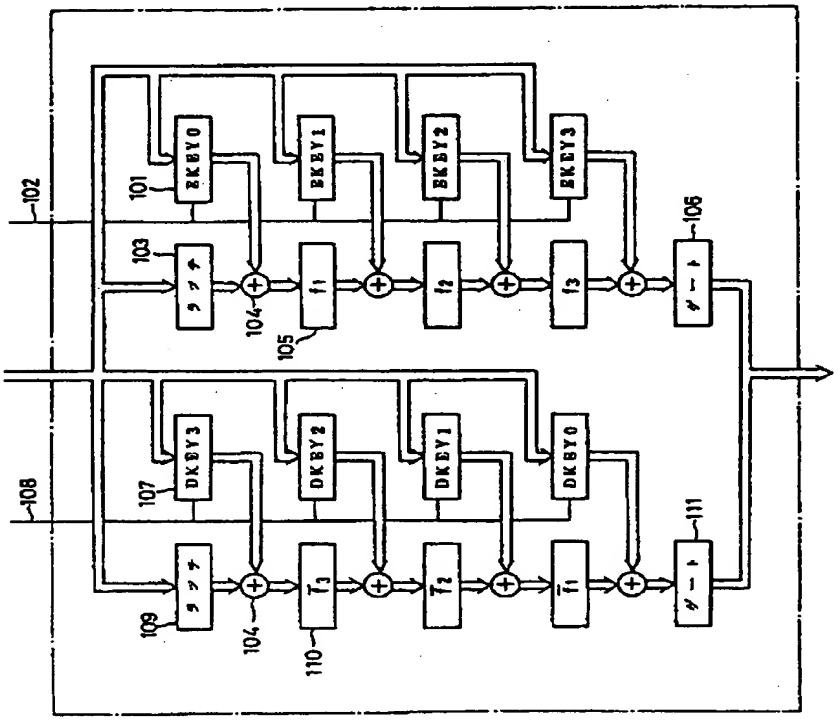


第2実施例の通信制御装置の構成図
第 8 図



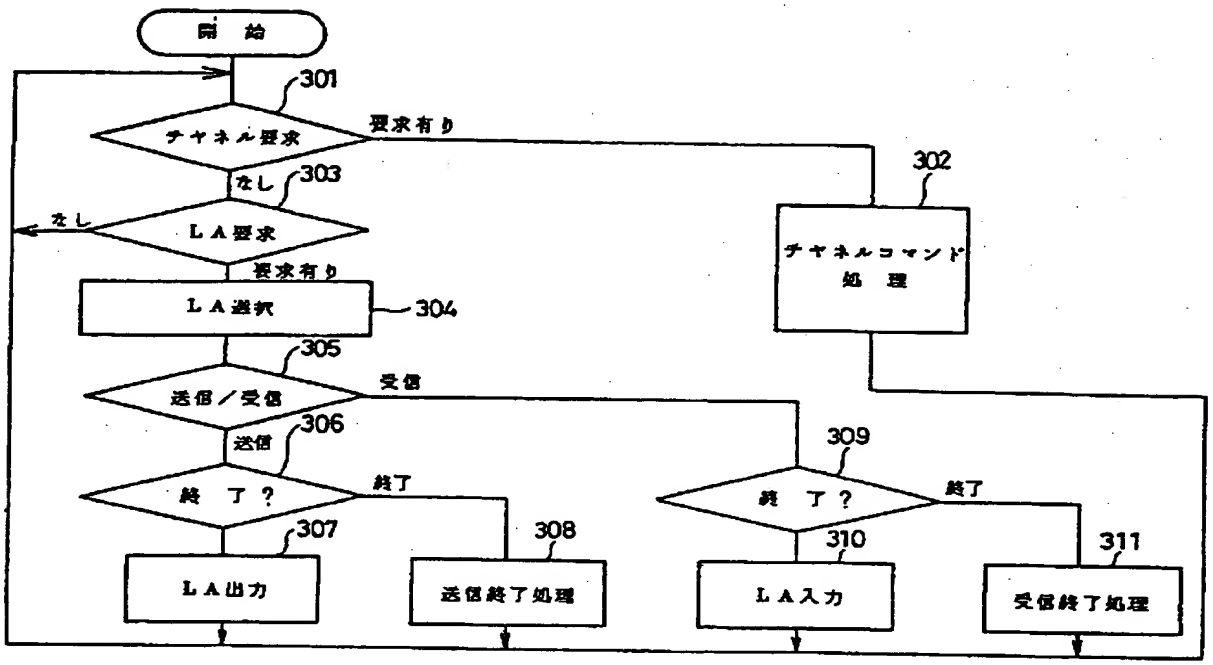
第8図におけるROMコントロールメモリの構成図

第 9 図



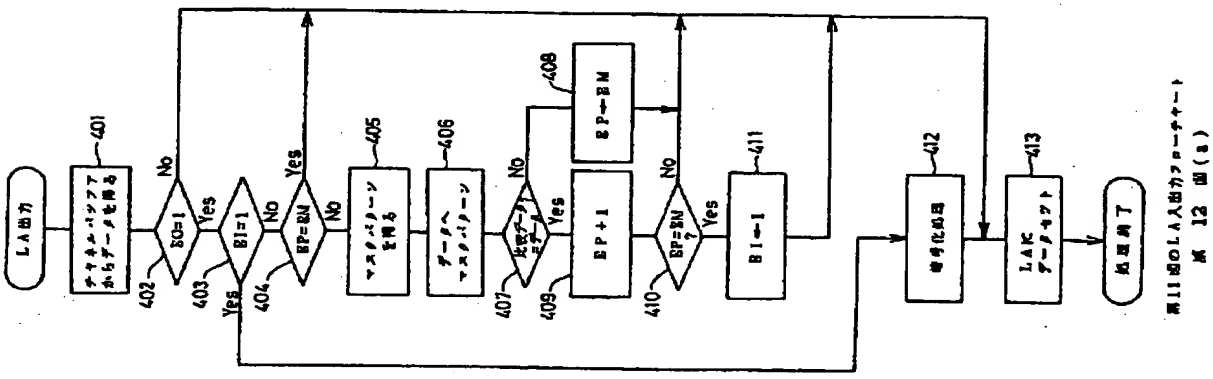
第8図のマック/ロック部の詳細構成図

第 10 図



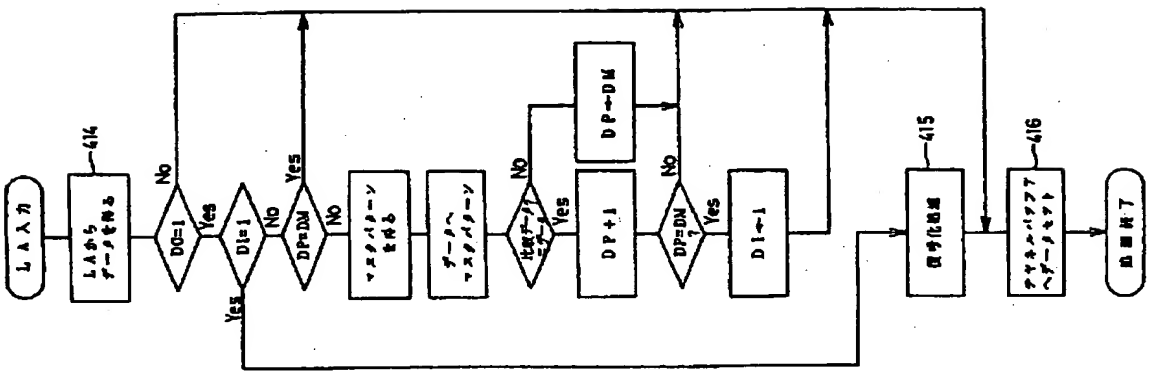
第８図の装置の制御フローチャート

第 11 図

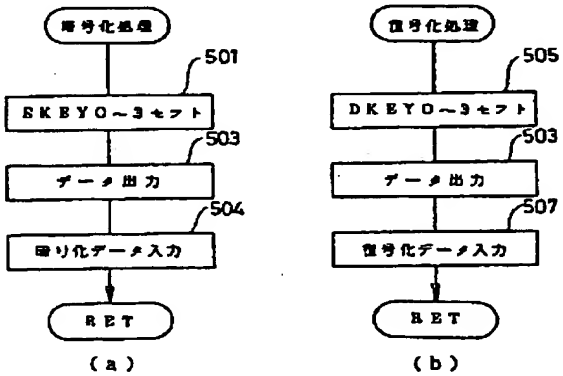


第11図のLA入出力フローチャート

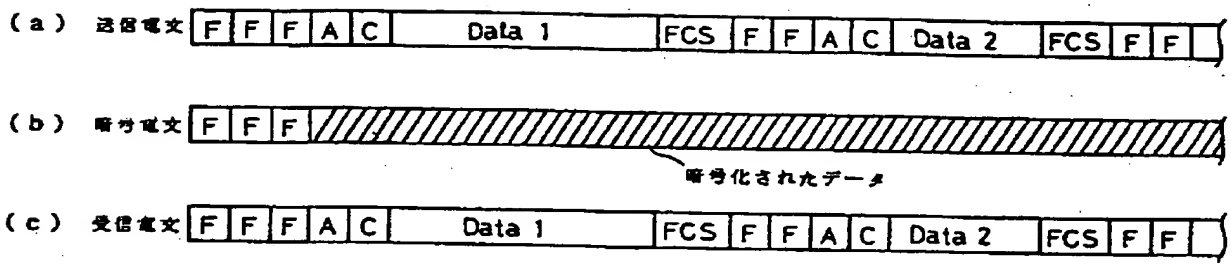
第 12 図(a)



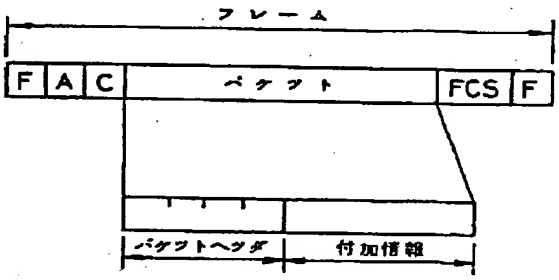
第11図のLA入出力フローチャート
第 12 図(b)



第12図の暗号化／復号化処理のフローチャート
第 13 図



従来の送受信電文と暗号電文の構成図
第 14 図



パケットの構成図
第 15 図